Cisco Catalyst 8000V Edge Router Performance Assessment

April 2021

DR210226F

Contents

1.0 Executive Summary

Virtualization of data center and their applications helps businesses become more cost efficient and flexible, using third-party service provider-hosted clouds to boost on-demand infrastructure and resources for more efficient operations.

While enterprises can surely benefit from this optimized level of service, it does pose a new mixture of networking and security issues. For instance, the enterprise no longer owns its cloud connectivity and cannot extend its network configuration to the cloud. Third-party cloud integration also eliminates previously hardened security and privacy seen on premise. Further, without direct connection from its distributed branch sites to the cloud applications, all network traffic must be backhauled through the data center.

Cloud providers experience their own challenges – such as limitations on scalability, Quality of Service (QoS), application visibility and Service-Level Agreements (SLAs).

Cisco offers its Catalyst 8000V Edge solution – a software router that either an enterprise or cloud provider can virtually deploy in a provider-hosted cloud or its own virtual environment. This solution gives the option of running on Cisco Unified Computing System (Cisco UCS) servers or any servers supporting VMware ESXi, Red Hat KVM virtualization; or on the Amazon EC2 cloud, Microsoft Azure cloud, or Google Cloud Platform (GCP). This router also contains the Cisco IOS XE software networking and security features and while addressing cloud-based networking and security constraints.

Using a real-world, cloud-based deployment of the Cisco Catalyst 8000V Edge SD-WAN solution, Miercom engineers demonstrated the following:

- Throughput in three public clouds
- Scalability in three public clouds
- SaaS M365 optimization
- Cisco Catalyst 8000V in Azure Virtual WAN Hub automation

Key Findings of the Cisco SD-WAN Solution

- **SD-WAN Performance.** Proved nearly 14 Gbps IPSec and 11 Gbps IQDF + NAT throughput for cEdge c5n.9xlarge instance using different cloud platforms, such as AWS, Google Cloud and Azure, with large frame and IMIX traffic.
- **Scalability in the Cloud.** Verified as many as 2,044 SD-WAN tunnels, 108,527 OMP Routes, 149,969 DPI Flows, and 149,916 cFlows with an average of 68% CPU and 9.7% RAM for AWS, Google Cloud and Azure cloud-based platforms.
- **SaaS Microsoft 365 Optimization.** Dynamically loads IP/URL Categorization signatures through SD-AVC & use Application Performance telemetry data received from Microsoft to select optimal path to the M365 Application.
- **Streamlined Customer Experience.** Cisco's partnership with Microsoft 365 offers more traffic control, improved speed, and higher efficiency for a suite of applications. Cisco's automation eliminates the configuration process for enhanced application usability.

- **Simplified SD-WAN Fabric Extension to the Cloud.** Complicated backend processes are made easy with a single user interface and configuration template to help customers, not experienced in the cloud platform (e.g. Azure) or SD-WAN, connect virtual branch networks to the SD-WAN Fabric via vHub/vWAN in just a few clicks – saving time and cost.

Based on our findings, the Cisco Catalyst 8000V Edge solution achieved or exceeded all advertised throughput, scalability and management specifications without incident, instability, or errors. We proudly certify the Cisco SD-WAN solution as **Miercom Performance Verified**.

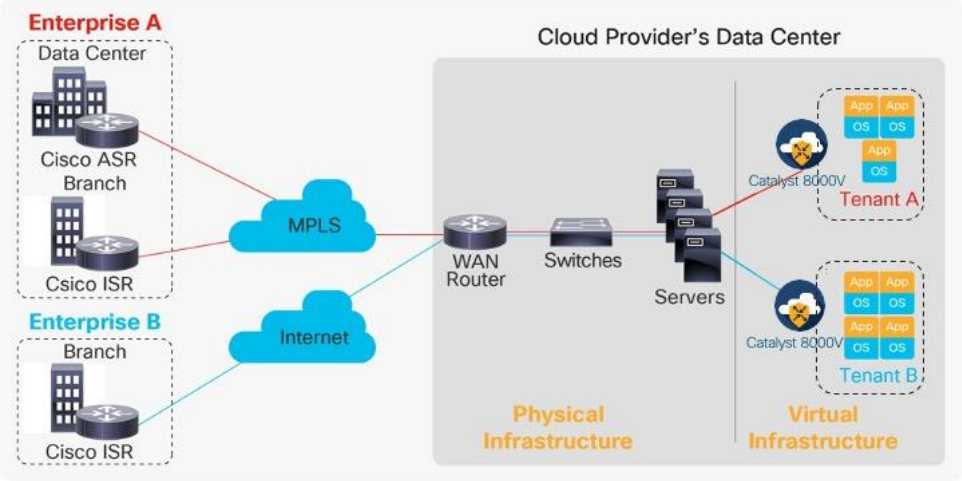
Robert Smithers

CEO, Miercom

2.0 Introduction

2.1 Cisco Catalyst 8000V Router

The Cisco Catalyst 8000V Edge is a virtual router that delivers SD-WAN, WAN gateway, and network services functions into virtual and cloud-based environments. Its industry-leading Cisco IOS XE software enables WAN extension into provider-hosted clouds, so even cloud providers themselves can use the Catalyst 8000V for enterprise-level networking to their customers.



Source: Cisco

A typical cloud provides IT infrastructure and resources to multiple customers or tenants. The Cisco Catalyst 8000V serves primarily as a router per tenant (Figure 1). That is, each tenant gets its own routing instance and hence, its own VPN connections, firewall policies, QoS rules, access control, and so on. The router can, however, also be deployed as a multitenant router, using Virtual Route Forwarding (VRF) to maintain separate routing tables and feature configurations for each tenant it services.

By using the same Cisco IOS XE Software platform as the Cisco Catalyst 8000 Edge Platforms Family, the Cisco Catalyst 8000V offers routing, VPN, firewall, Network Address Translation (NAT), Quality of Service (QoS) application visibility, failover, and WAN optimization.

Cisco Catalyst 8000V Virtual Machine Specifications

Virtualized Server Hardware	Description
CPU	1 to 8 vCPU on ESXi/KVM hypervisor, up to 16 vCPU on public cloud instance (depending on throughput and feature set)
Memory	4 to 16 GB (depending on throughput and feature set)
Disk Space	8 GB or 16GB
Network Interfaces	1+ vNICs, up to maximum allowed by hypervisor

2.2 Cisco Software-Defined WAN (SD-WAN)

Cisco SD-WAN connects branch networks, users, devices and cloud deployments over a set of secure WAN links via routers, such as the Catalyst 8000V, for optimized service and heightened application experience. Customers can exert control over performance, bandwidth, security and availability of WAN links using this intelligent Cisco SD-WAN software.

The Catalyst 8000V offers enhanced application performance and reliability at reduced costs using Cisco SD-WAN. Its deep packet inspection can identify and control thousands of applications. With Cisco SD-WAN, the Catalyst 8000V can manage end devices, in the cloud or on-premise, based on throughput-based subscription licenses. Subscriptions include: Cisco DNA Essentials, Cisco DNA Advantage, and Cisco DNA Premier.

- **Cisco DNA Essentials:** connectivity and router life cycle management, network and application visibility, basic premise and transport security
- **Cisco DNA Advantage:** advanced WAN topologies, application-aware policies, enhanced network security
- **Cisco DNA Premier:** cloud connectivity, unlimited segmentation, advanced application optimization, network analytics, advanced threat protection security

For more information on Cisco SD-WAN subscriptions, please refer to:

https://www.cisco.com/c/en/us/products/software/one-wan-subscription/index.html.

Customers benefit from SD-WAN by extending their SD-WAN fabric to cloud deployments, serve business-critical applications on a best-effort basis, and use multiple paths for highly reliable service. Costs are significantly reduced by replacing dual MPLS links with a mixture of MPLS and Internet links and by minimizing time-to-deploy new remote sites by supporting rapid DSL and 3G/4G LTE connections. Security across connections is ensured with zero-touch VPN technology.

2.3 The Cisco IOS XE Software Advantage

Cisco IOS XE Software allows the Cisco Catalyst 8000V to provide control-plane and data-plane separation, multicore forwarding, and flexible architecture for optimized, dynamic cloud environments.

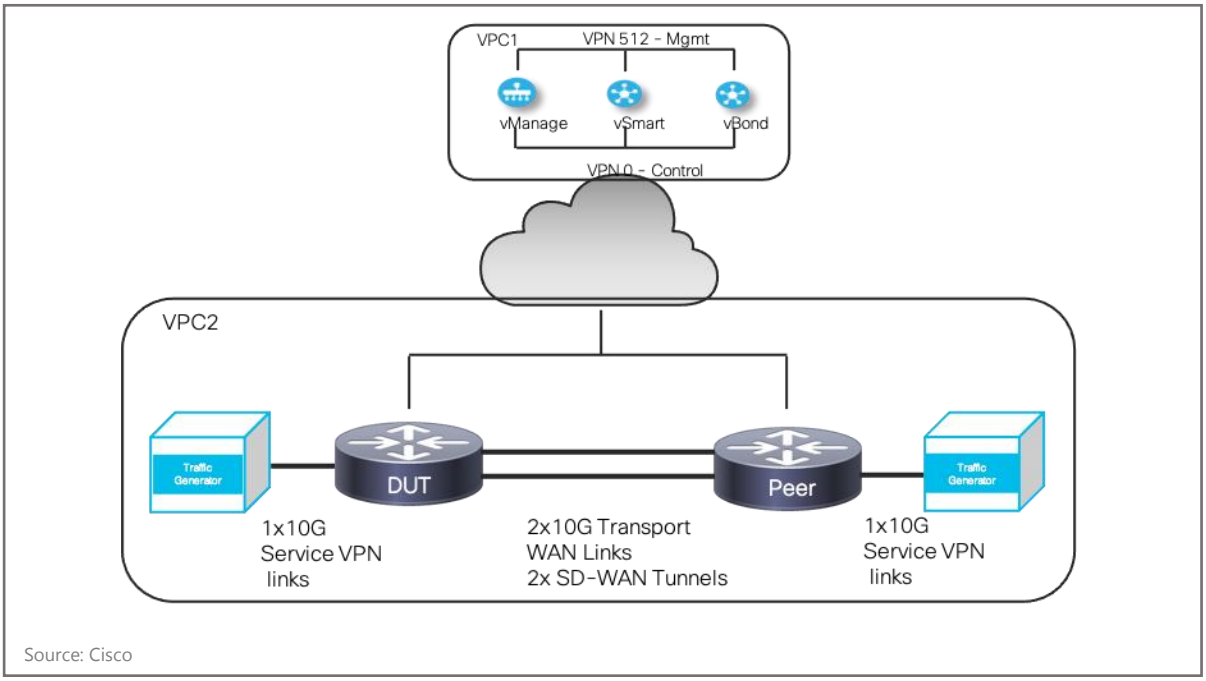
Some key benefits of Cisco IOS XE Software include:

- Proven networking and security features – as previously seen in Cisco Integrated Service Routers (ISRs) and other hardware routers in enterprise, service provider and government networks
- Efficient operation and rapid integration of branch office, WAN, data center and cloud
- Quality controlled experience with legacy Cisco IOS Command-Line Interface (CLI) and management tools (across the Catalyst 8000 Edge platforms)

3.0 How We Did It

Miercom participated in hands-on testing with a real-world network environment simulated by industry leading traffic generation tools for a realistic assessment of performance. The following topology was used.

Test Topology



The topology above depicts how the Cisco Catalyst 8000V was deployed to test SD-WAN throughput in three public clouds: AWS c5n.9xlarge, GCP N1-standard-8, and Azure F32.

Device under Test (DUT)	
Cisco Catalyst 8000v	Version 17.04.01.0.211
Traffic Generator Descriptions	
Spirent Test Center	Version 5.16.0166.0000 A high-speed test tool to generate traffic flows and routes emulation to validate the scalability of the platform in this test.
TRex	Version 2.79 An open source traffic generator used to validate the throughput performance in this test. https://trex-tgn.cisco.com

4.0 Performance

Security requires high-quality services that typically will negatively affect network performance. Router solutions that provide security aim to minimize processing to maintain competitive performance by finding an optimal balance.

Our testing intended to validate the performance throughput incurred while protected by Cisco Catalyst 8000V Edge SD-WAN rich features.

The TREX test tool generated 100 servers and 1,000 clients to simulate 1,000 one-to-many flows of bi-directional traffic with randomized IP addresses. The test duration was 120 seconds, measuring aggregate throughput with Partial Drop Rate (PDR) of 0.01 percent frame loss.

We used IPv4 unicast traffic with 1400 bytes packet size. Packet size is defined as Ethernet frame size: Ethernet Header (DMAC/SMAC/EtherType) + Ethernet FCS + IP Header.

The SD-WAN solution was tested using throughput profile of feature combinations of Internet Protocol Security (IPsec), Quality of Service (QoS), Deep Packet Inspection (DPI), Netflow, Network Address Translation (NAT):

1. IPsec + QoS +DPI + Netflow + NAT (a.k.a IQDF +NAT)

The Cisco XE SD-WAN solution used the controller version 20.4 and Catalyst 8000V image version 17.4.1a.

This test was performed on three different cloud platforms:

Cloud Instances	vCPU	RAM
Amazon Web Services (AWS) c5n.9xlarge	36	96GB
Google Cloud Platform (GCP) N1-standard-8	8	30GB
Azure Cloud F32	32	64GB

What We Expect

The Catalyst 8000V should provide aggregated SD-WAN IQDF+NAT throughput of more than 10Gbps in AWS C5n.9xlarge, more than 2Gbps in GCP N1-standard-8 and more than 6Gbps in Azure F32 instance while ensuring no bottlenecking occurs on supporting devices.

Results

Cisco XE SD-WAN IQDF + NAT Performance (Gbps)

Observed	AWS c5n.9xlarge	GCP N1-standard-8	Azure F32
1400 byte	10.4 Gbps	2.38 Gbps	6.91 Gbps

* IQDF+NAT represents common services in SD-WAN deployment in the public cloud.

5.0 Scalability in the Cloud

Networks are designed based on the demands placed by the products and services – for both the current intent and the future. SD-WAN solutions are expected to be flexible in terms of scale in multi-dimensional, the following tests are conducted with all features (SD-WAN Tunnels, OMP Routes, DPI flows, cFlows) to scale up simultaneously to reflect the real-world deployment scenarios.

The DUT tested for SD-WAN scalability in the public cloud by sending traffic streams through the router and SD-WAN Fabric to three different cloud-based services: Amazon Web Services (AWS), Google Cloud Platform (GCP) and Azure.

The number of flow entries were observed and recorded. These results were intended to verify design specification as advertised by Cisco scalability claims.

The following features were enabled for this series of tests:

- SD-WAN Tunnels
- DPI (Deep Packet Inspection)
- cFlow
- OMP Routes

Results

Scalability Testing Summary

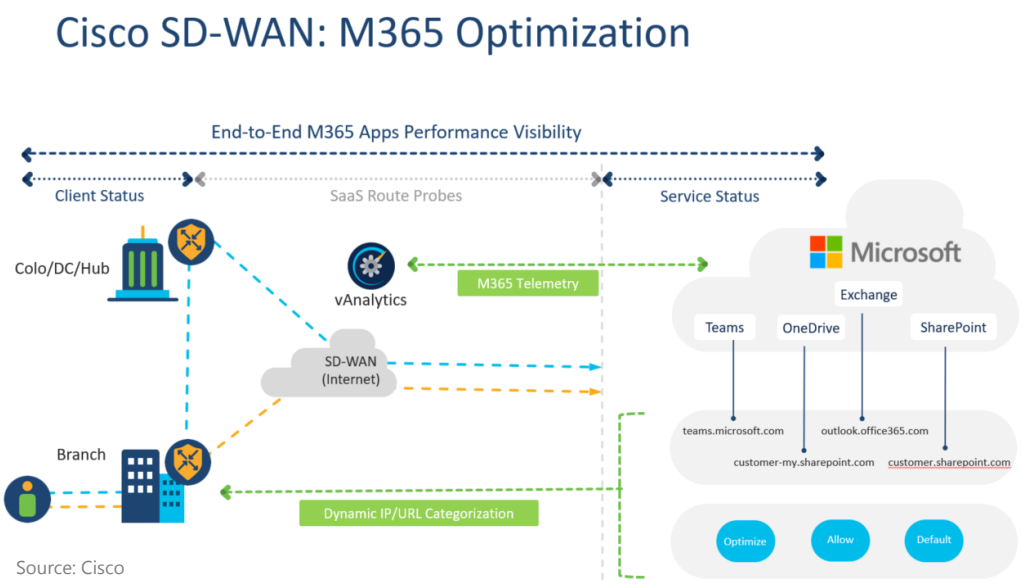
Features	AWS c5n.9xlarge	GCP N1-standard-8	Azure F32
SD-WAN Tunnels Observed	**2,034**	**2,044**	**2,038**
OMP Routes Observed	**108,517**	**108,527**	**108,513**
DPI Flows Observed	**148,703**	**149,429**	**149,969**
cFlows Observed	**149,742**	**148,691**	**149,916**

6.0 SaaS Microsoft 365 Optimization

Cisco SD-WAN's Cloud OnRamp solution for Software-as-a-Service (SaaS) optimizes the user experience for applications by probing and measuring path performance and dynamically selecting optimal path for forwarding SaaS traffic. Cloud-based computing has its challenges, but Cisco and Microsoft collaborated to develop new features intended to improve integration of Cisco SD-WAN OnRamp for SaaS and Microsoft 365. Such improvements include: controllable traffic flow, insightful metrics, automated policy integration, and robust user experience.

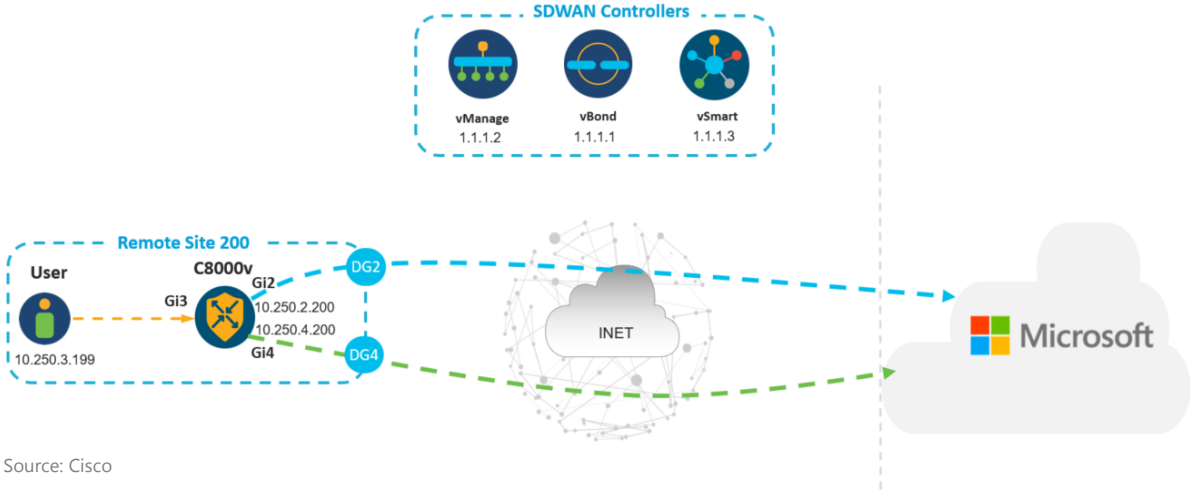
This collaboration is based on the following:

1. **Dynamic IP/URL Categorization.** Microsoft 365 has suite of applications (e.g., Exchange, Teams, SharePoint) whose traffic would require preferential treatment. Each of the endpoints associated with these applications have their own tolerance level for loss, latency, and jitter, as well as different requirements for security and monitoring based on different levels of trust. Based on this, Microsoft introduced categorization dividing M365 traffic into 3 categories, namely: Optimize, Allow and Default. Cisco SD-WAN downloads this IP/URL signatures directly from Microsoft. This helps in classifying the M 365 traffic, and securely forwarding through a preferred path. This direct download yields better performance, security, and optimizes user experience.
2. **Informed Network Routing (end-to-end application performance visibility).** Microsoft provides contextual and insightful performance metrics for visibility into application performance in addition to network performance. Cisco SD-WAN uses this application telemetry data along with its probing telemetry data to dynamically select the best path for M365 traffic.



Microsoft plays a critical role in the telemetry-based decision making for optimized routing used by the cEdge routers on-site via vAnalytics. Telemetry Data is collected from both Microsoft 365 and vManage for a robust computation of the best performance routing approach.

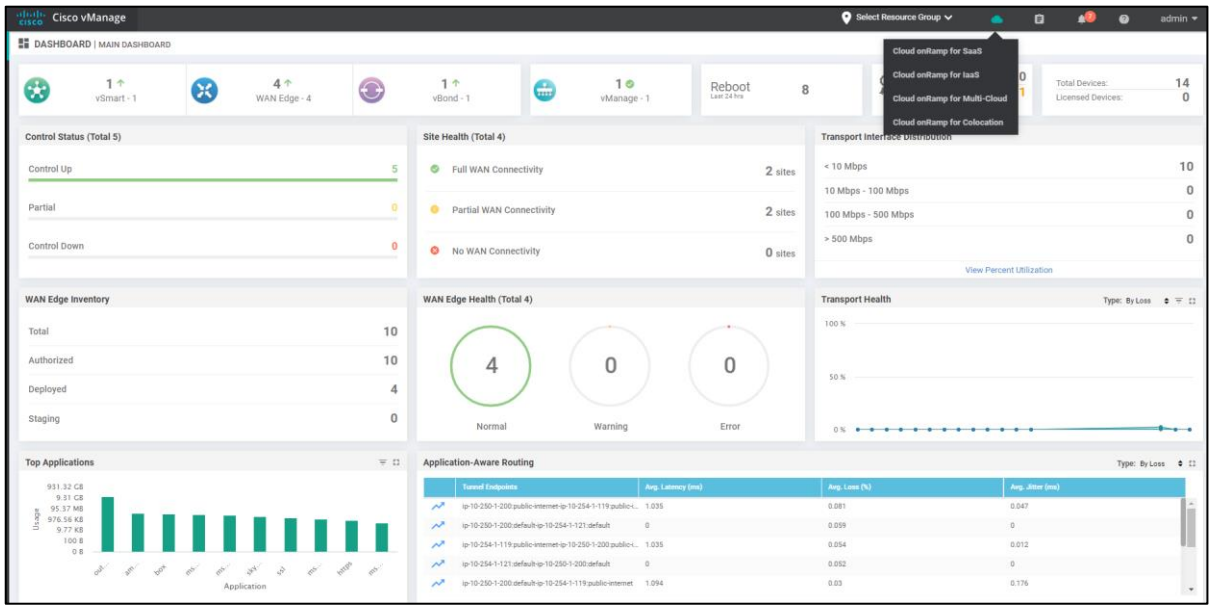
The intention of our test was to demonstrate the new capability of M365 telemetry, with multiple paths to the M365 Cloud. By probing an egress point, we observed how M365 sends telemetry data for an Exchange application to vAnalytics. vAnalytics runs its algorithm and propagates best-path recommendation to the Catalyst 8000V Edge devices to reach Exchange application.



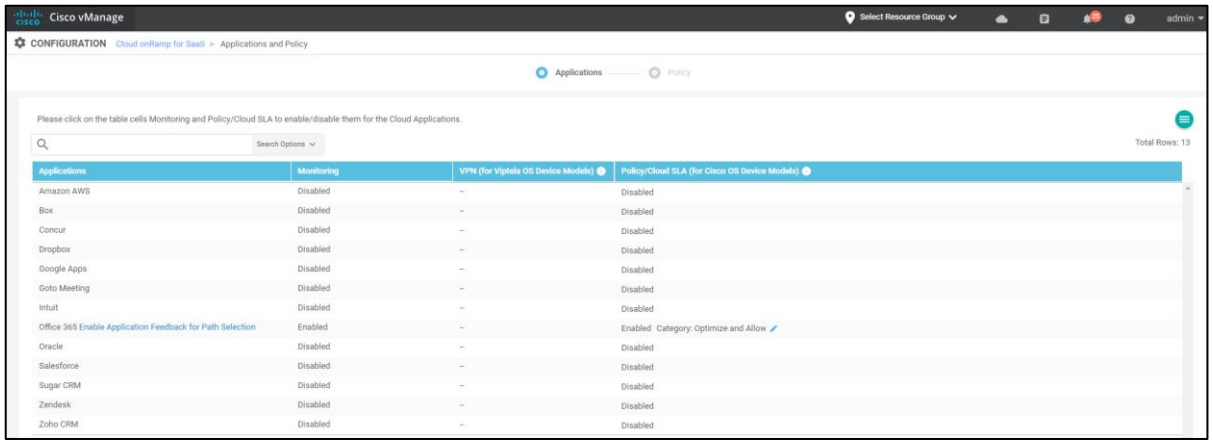
Source: Cisco

6.1 Dynamic IP/URL Categorization

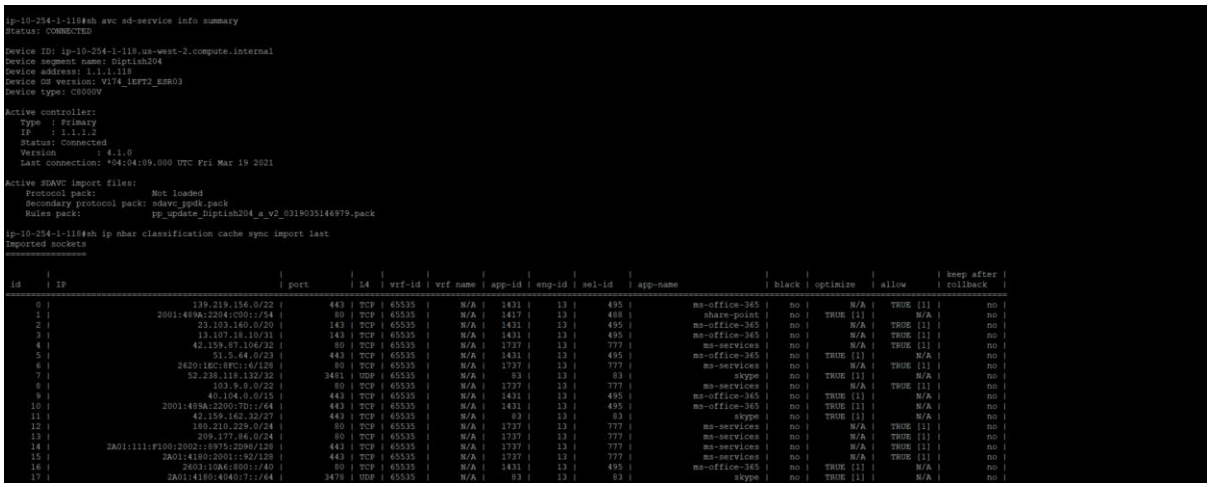
We observed the SD-AVC (Software Defined Application Visibility and Control) reaches out, downloads the IP/URL categorization signatures, and keeps it updated.



Cisco vManage is where customers can configure the Dynamic IP/URL Categorization feature, by selecting "Cloud OnRamp for SaaS" from the drop-down menu of the cloud icon and selecting "Application and Policy".



Cisco supports many SaaS applications, so by selecting Microsoft 365 from the list, we can configure the application and its policies. Here customers have the option to enable both IP/URL Categorization and Telemetry Exchange for Informed Network Routing. Under the "Category" option, you can specify which category of traffic to prioritize (e.g., Optimize and Allow, Optimize, All). Next to the application, we saw an option to "Enable Application Feedback for Path Selection". This needs to be enabled to exchange telemetry data. Customers have the option to simply enable Dynamic IP/URL categorization only or enable both IP/URL Categorization and Telemetry Exchange for Informed Network Routing.



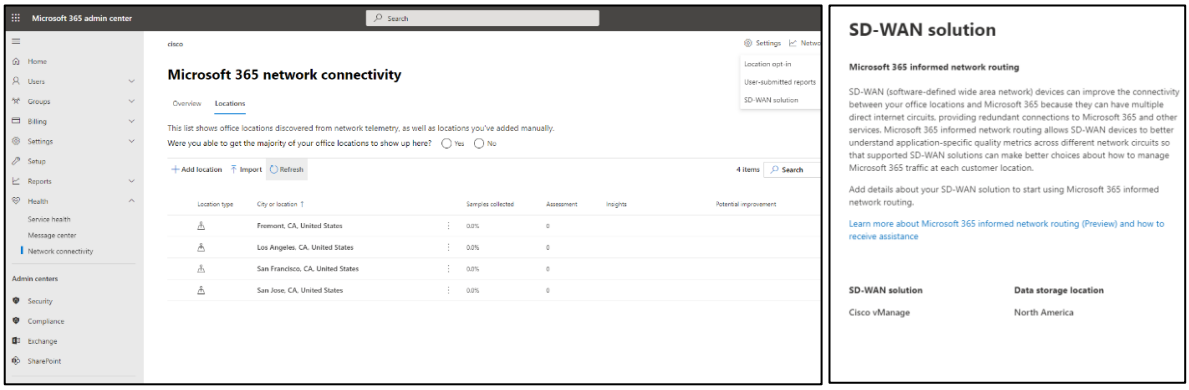
We saw how this SDAVC connections look in the cEdge router using PuTTY terminal. We see a list of IP addresses and whether Optimize, Allow, or Default is enabled (TRUE).

Since the cEdge (c8000v) has the verified list of M365 endpoints, these IP addresses traffic can be securely routed through a preferred DIA (Direct Internet Access) thus leading to reduced latency, increased performance, and decreased cost.

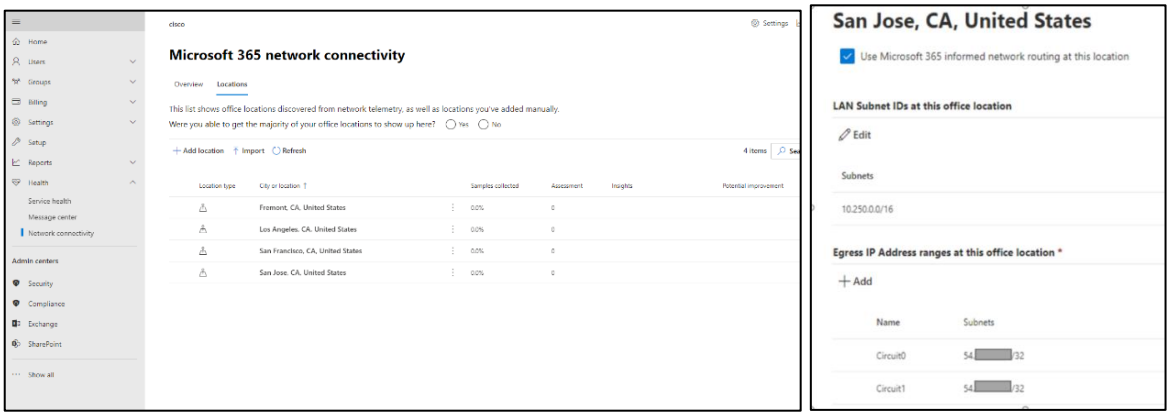
6.2 Informed Network Routing

Cisco's vAnalytics Engine receives path probing telemetry data from vManage and application performance telemetry data from Microsoft. vAnalytics runs its algorithm based on this data and backfeeds the best-path recommendation to the cEdge router (c8000v). The cEdge router polls the vAnalytics every 5 minutes and downloads the recommendation.

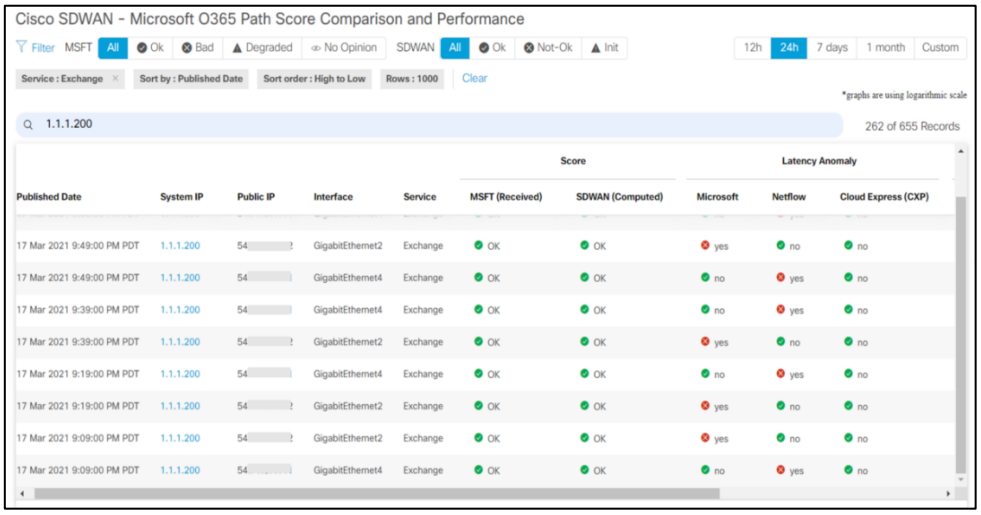
Likewise, vAnalytics periodically sends Cisco Telemetry data to Microsoft. Microsoft may use this data to debug or troubleshoot application performance.



To set up from the Microsoft end, we used the Microsoft Admin Portal > Health > Network connectivity > Settings > SD-WAN solution. We observed Cisco vManage was set up as the SD-WAN solution; Cisco is the only vendor that supports this capability for Microsoft 365.



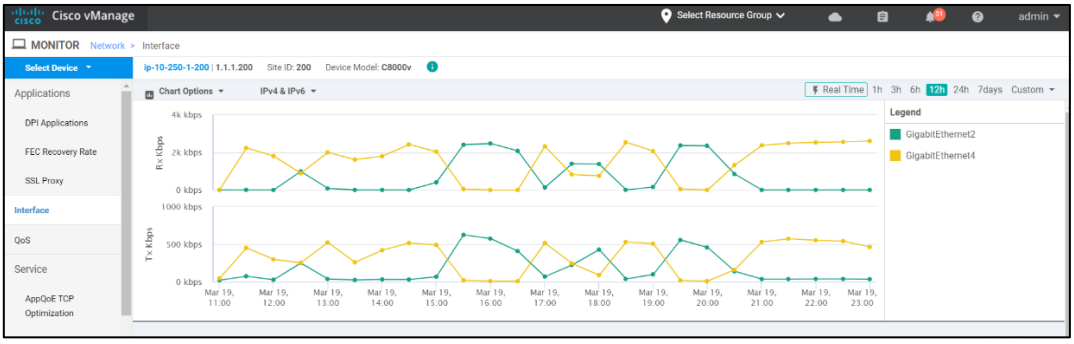
We then were able to enable to branch networks. By selecting a branch, we were able to enable WAN circuits (Internet connectivity) to the Edge devices. For vAnalytics/vManage and Microsoft 365 to exchange data on the best path, we need to only configure IP addresses for these WAN circuits.



Cisco SD-WAN vAnalytics instance is hosted in the cloud, independent of vManage and SD-AVC. Under Path Score, we can see the WAN links used from the cEdge router to Microsoft 365. This information is visible for windows of 12 hours, 24 hours, 7 days, or 1 month.

```
ip-10-250-1-200#sh sdwan cloudexpress service-area-applications
cloudexpress service-area-applications Exchange vpn 1 office365
 exit-type       local
 interface       GigabitEthernet2
 latency         13
 loss            0
 override-status OK
cloudexpress service-area-applications Skype vpn 1 office365
 exit-type       local
 interface       GigabitEthernet2
 latency         68
 loss            0
 override-status OK
```

We looked at the paths to the Internet from the c8000v router. We see that Microsoft splits applications into service areas (e.g. Exchange, Skype, Teams). Application over routing" identifies an application, such as Exchange, and routes it to a specific interface. vAnalytics's recommendation takes priority in deciding the best-path for forwarding M365 traffic. If vAnalytics's recommendation is not conclusive than it reverts back to Cloudexpress, which is Cisco SD-WAN's path probing mechanism.



Links are analyzed for performance over time to make informed decisions on whether that link is optimal or not. We see that M365 traffic is switching across the 2 available paths based on their performance over time.

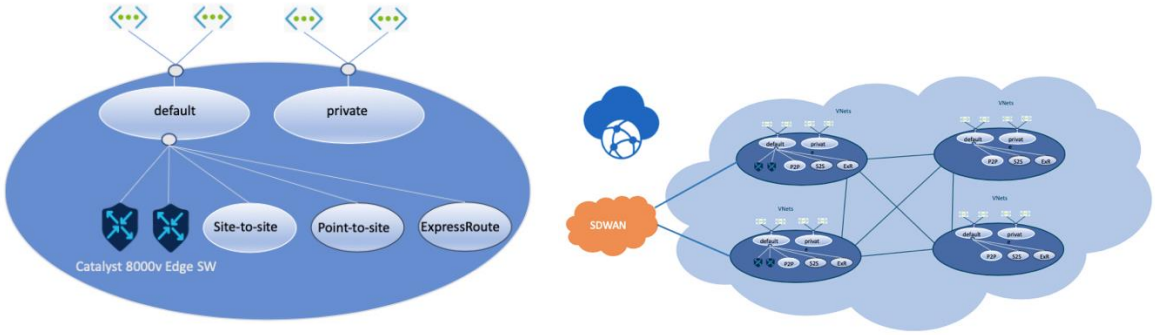
We found that Cisco's partnership with Microsoft 365 offers a significantly streamlined customer experience with more control over traffic, improved speed and efficiency for a suite of applications. By using automation, Cisco SD-WAN was found to eliminate the configuration process for a more useful application experience.

7.0 Catalyst 8000V in Azure Virtual WAN Hub Automation

We looked at how Cloud OnRamp (CoR) for MultiCloud extends SD-WAN connectivity to Azure Virtual Hub (vHub) and Virtual WAN (vWAN). This model automates the creation of 2 Catalyst 8000V edge devices inside a regional virtual hub with direct BGP peering to the (vHub) router. This architecture eliminates the need for IPSec tunnels to an Azure VPN Gateway. CoR automation shields the user from the complexities of both the cloud platform and SD-WAN.

vHub/vWAN are vital constructs of Azure networking, allowing for scalability, segmentation, and global peering across the Azure Backbone. vHubs are regional termination points for site-to-site, point-to-site and ExpressRoutes connections as well as hosting our Catalyst 8000V. Routes are exchanged using BGP peering. A virtual WAN is a logical grouping of one or more vHubs. vHubs within a VWAN are globally peered in a full mesh topology and exchange routes automatically.

For this test, we used CoR to extend the SD-WAN Fabric into the vHub, effectively making Azure look like another customer branch site.



Source: Cisco

The two Catalyst 8000V Edges created inside the vHub act as tunnel termination endpoints for other branch sites. The vWAN is then a collection of these vHubs with global transit regional gateways that all access the SD-WAN fabric, where each region is just one hop away from another. These regions – or VNets – talk to each other via vWAN and have distributed route tables to do this.

Using Cisco's Cloud OnRamp in vManage, we setup the SD-WAN cloud connections with Azure to discover, manage and create intent.

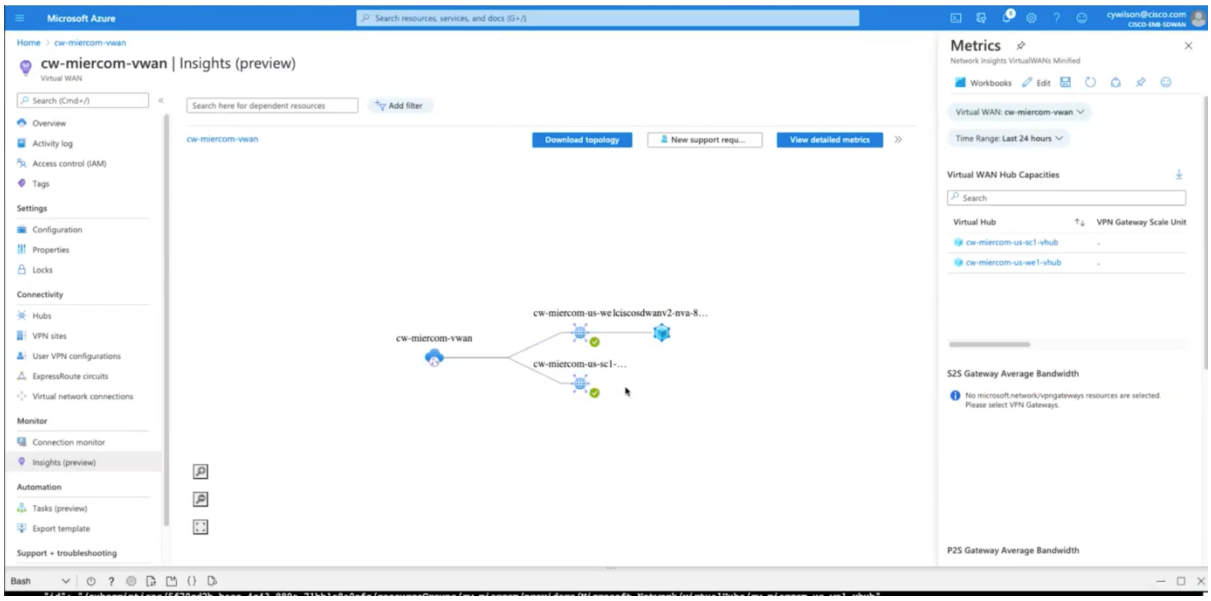
The objective of this test was to show vWAN workflow and automation using the Catalyst 8000V Edges in the vHub. Testing consisted of three workflows:

1. Create Cloud Gateway
2. Discover and Tag VNets
3. Declare Intent

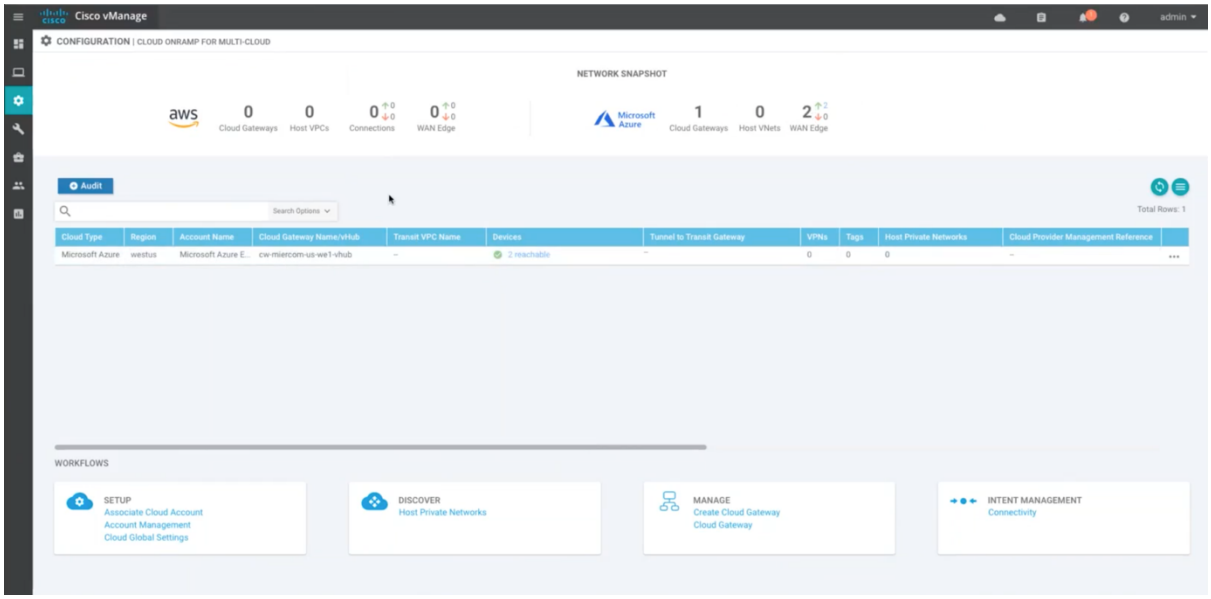
7.1 Create a Cloud Gateway

We first created a Cloud Gateway using Microsoft Azure and the two Catalyst 8000V Edges. We create a vWAN and vHub, along with network virtual appliances, and register with the control plane to make Azure part of the SD-WAN Fabric.

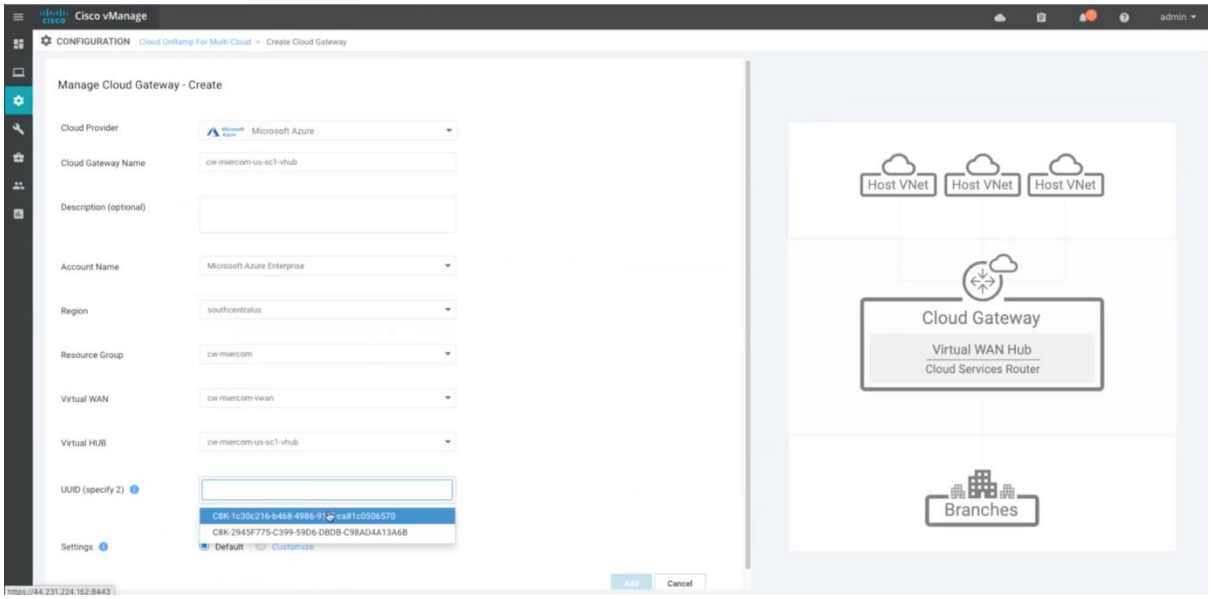
We started by authenticating Azure's subscription ID, active directory ID, application client ID, and application security key. Using Cisco vManage we then assign a "role" to Azure.



In vHub > Virtual Network Connections, we saw VNets are currently not connected to the vHub/vWAN. The topology consists of a vWAN component, two VNets (to be connected), and a vHub (made using two Catalyst 8000V Edges).



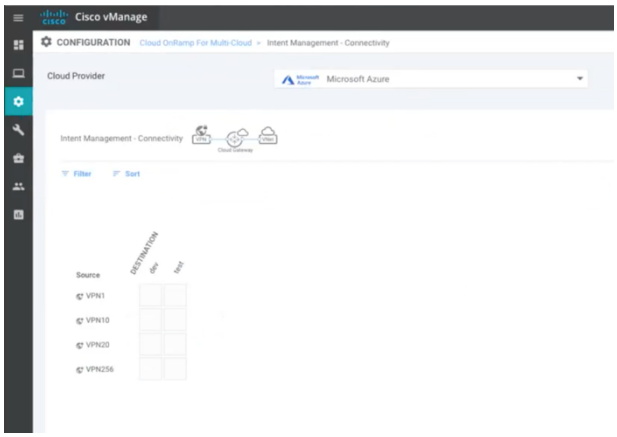
In the vManage dashboard, we use either the cloud icon in the top-right corner or Configuration > Cloud OnRamp for Multi-Cloud to create a configuration. We saw two WAN Edges since there is a WAN pair (Catalyst 8000V Edges) per WAN Gateway. At the top we observed that there was currently one Cloud Gateway, no Host VNets and 2 WAN Edges. The purpose of the workflow was to setup and connect these Host VNets (branches) to the vHub.



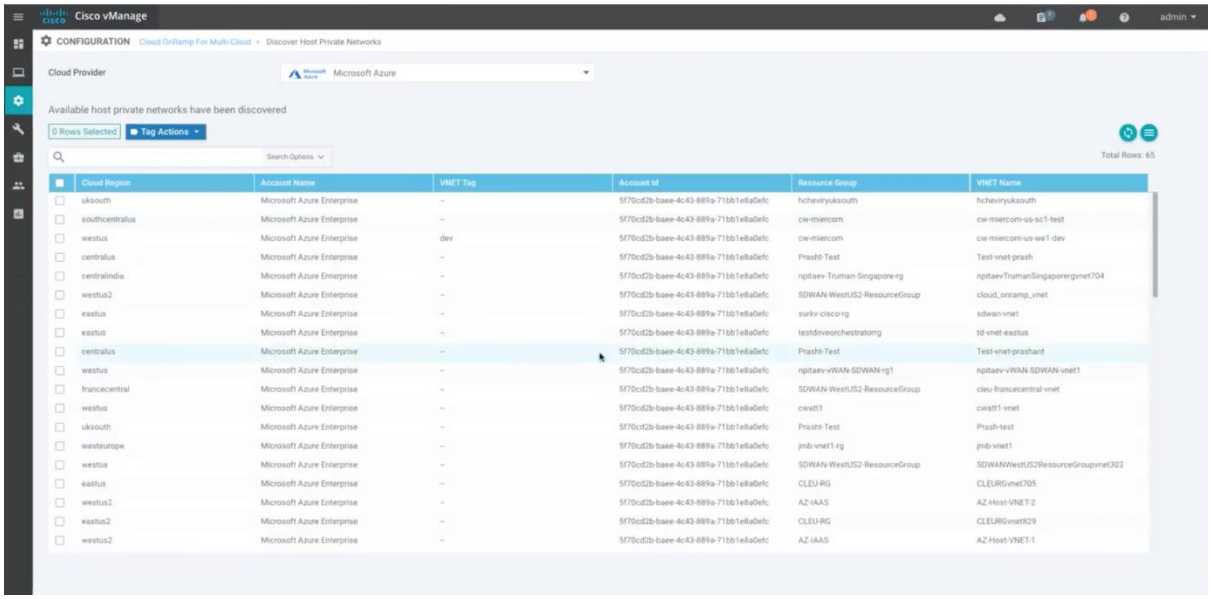
We created a Cloud Gateway using a configuration template, which used default settings that attached devices by Hostname(s), System IP and Site ID. This configuration could be scheduled to push to the Catalyst 8000V Edges via "blob storage" and inserted into the devices at bootup. These devices are then registered with the control plane to extend the SD-WAN control plane fabric.

7.2 Discover and Tag VNets

Once we assume the role of Azure, we create visibility into the VNets by tagging. Tagging gives a logical representation of the VNets (e.g. "Test" VNet, "Dev" VNet) with an API to discover and tag.



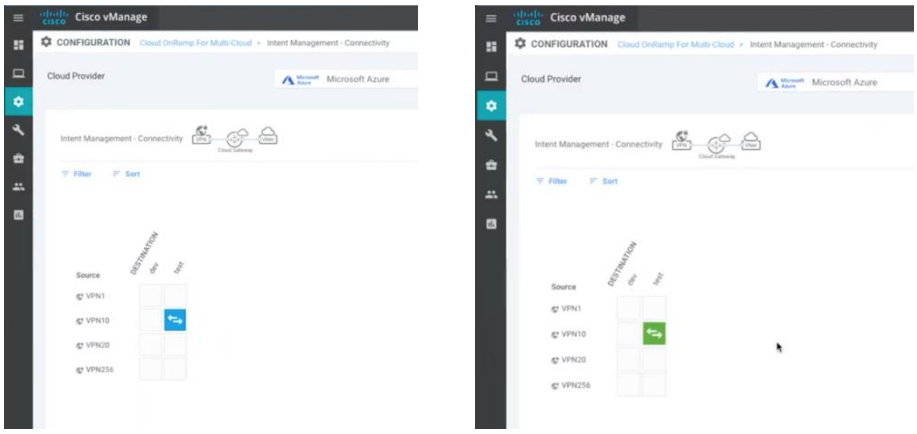
Under Cisco vManage Intent Management > Connectivity, we saw no connectivity in Azure before the VNets were successfully connected to the vHub.



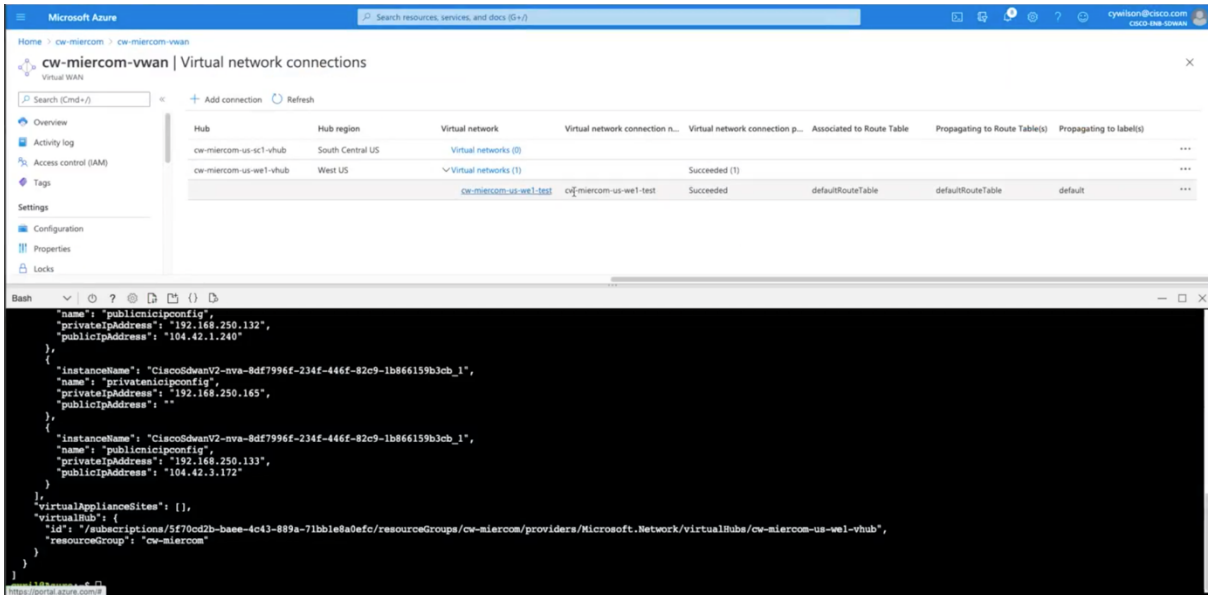
Under Discover > Host Private Networks, we see a list of all VNets. Here we can create a tag (in this case, we created a “test” tag) to logically group VNets.

7.3 Declare Intent

Declaring intent determines which VNet (by tag) needs to be connected to the vHub in order to grant access. We do this by first authenticating, assigning a role, establishing the VNet connection to the vHub, and pushing the configuration from the template to the created Virtual Routing and Forwarding (VRF) for connectivity. Creating a vHub takes approximately 30 to 40 minutes, but the rest is just a couple clicks to connect.

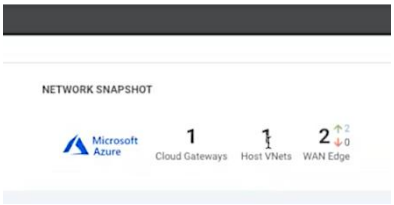


We created intent by assigning connectivity to the vHub using VPN10. In Cisco vManage, we saw Azure successfully connected the VNet to the vHub via VPN10 when the icon turned from blue to green. This was also confirmed by SSH access into the VPN10, like any other network device.



We also observed this connection was successful in Azure. The VNet we tagged was successfully connected to the vHub, and it was automatically associated to the Route Table and propagated to the Route Table(s) and label(s) with just a couple clicks.

We then saw the Host VNet count went from 0 to 1 in the Cloud OnRamp interface. This verified we had access to the Cloud Gateway (one vHub per region that we created) and one of the Host VNets through two of the High Availability (HA) WAN Edge links (supported by two Catalyst 8000V Edges inside the vHub that access the Host VNet).



Once we declared intent, we automatically have updated the template configuration via tunnelling for creating BGP routes, neighbor commands, quick routing policies, and VRF policy. As opposed to a typical branch where the customer would have to create a service VPN, this is automatically created when declaring intent. This ensures BGP routing from the VRF to the vHub, effectively controlling access. In this case we used VRF10, and this is the only VRF with permission to access the vHub. Unless we also grant this access to, for example, VRF20, it will not have access to the vHub. This is all set up with just one click in vManage.

While there were a lot of complicated backend processes involved in via API calls between Cisco vManage and Azure, the customer can accomplish extending the SD-WAN Fabric with a single user interface and default configuration template. They need not be an expert in either Azure or SD-WAN to connect branch networks to the vHub for cloud integration of the SD-WAN Fabric. This can all be executed with a few clicks, saving time and cost.

About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable™, Certified Reliable™, Certified Secure™ and Certified Green™. Products may also be evaluated under the Performance Verified™ program, the industry's most thorough and trusted assessment for product usability and performance.

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report, but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

By downloading, circulating or using this report this report in any way you agree to Miercom's Terms of Use. For full disclosure of Miercom's terms, visit: https://miercom.com/tou.